CLAIMS

1. Method of making the execution of a computer program secure, the method being characterized in that it includes:

- a step of stacking a predetermined value in an instruction stack of the program; and
- a step of unstacking said stack adapted, where appropriate, to detect an execution anomaly.

2. Method according to claim 1, characterized in that said stacking and unstacking steps are respectively associated with elements of at least one subset of instructions of said program.

3. Method according to claim 2, characterized in that said elements are respectively an opening bracket and a closing bracket in a system of brackets.

4. Method according to claim 2, characterized in that said unstacking step is associated with a return instruction of said program or a subroutine of said program.

5. Method according to any one of claims 1 to 4, characterized in that said program is written in a programming language including a first instruction whose execution implements said stacking step and/or a second instruction whose execution implements said unstacking step.

6. Method according to claim 5, characterized in that the second instruction terminates said program or a subroutine of said program.

7. Method according to any one of claims 1 to 6, characterized in that said predetermined value is representative of a subset of critical instructions of said program.

8. A method according to any one of claims 1 to 7, characterized in that it includes an anomaly processing step executed if, during said unstacking step,

a value other than said predetermined value is unstacked.

9. Method according to any one of claims 1 to 8, wherein said program includes at least one call to a subroutine, characterized in that said stacking step is effected before said call and said predetermined value is eliminated from said stack during execution of said subroutine.

10. Method according to claim 9, characterized in that said predetermined value is the address of an anomaly processing function.

11. Method according to any one of claims 1 to 8, wherein said programming includes at least one call to a subroutine, characterized in that said stacking step is effected during execution of said subroutine and said predetermined value is eliminated from said stack after execution of said subroutine.

12. Method according to claim 11, characterized in that said predetermined value is the address of an anomaly processing function.

13. Information medium readable by a computer system, and where appropriate totally or partially removable, in particular a CD-ROM, or a magnetic medium, such as a hard disk or diskette, or a transmissible medium such as an electrical or optical signal, characterized in that it includes instructions of a computer program for implementing a method according to any one of claims 1 to 12 when that program is loaded into and executed by an electronic data processing system.

14. Computer program stored on an information medium, said program including instructions for executing a method according to any one of claims 1 to 12 when that program is loaded into and executed by an electronic data processing system.

15. Electronic entity that has been made secure

characterized in that it includes means for implementing a method according to any one of claims 1 to 12.

16. Electronic entity according to claim 15 characterized in that it is a smart card.